AN EXPLICIT ALGEBRAIC FAMILY OF GENUS-ONE CURVES VIOLATING THE HASSE PRINCIPLE

BJORN POONEN

ABSTRACT. We prove that for any $t \in \mathbf{Q}$, the curve

$$5x^3 + 9y^3 + 10z^3 + 12\left(\frac{t^{12} - t^4 - 1}{t^{12} - t^8 - 1}\right)^3 (x + y + z)^3 = 0$$

in $\mathbf{P}^2$ is a genus 1 curve violating the Hasse principle. An explicit Weierstrass model for its Jacobian E_t is given. The Shafarevich-Tate group of each E_t contains a subgroup isomorphic to $\mathbf{Z}/3 \times \mathbf{Z}/3$.

1. INTRODUCTION

One says that a variety X over $\mathbf{Q}$ *violates the Hasse principle* if $X(\mathbf{Q}_v) \neq \emptyset$ for all completions $\mathbf{Q}_v$ of $\mathbf{Q}$ (i.e., $\mathbf{R}$ and $\mathbf{Q}_p$ for all primes p) but $X(\mathbf{Q}) = \emptyset$. Hasse proved that degree 2 hypersurfaces in $\mathbf{P}^n$ *satisfy* the Hasse principle. In particular, if X is a genus 0 curve, then X satisfies the Hasse principle, since the anticanonical embedding of X is a conic in $\mathbf{P}^2$.

Around 1940, Lind [Lin] and (independently, but shortly later) Reichardt [Re] discovered examples of genus 1 curves over $\mathbf{Q}$ that violate the Hasse principle, such as the nonsingular projective model of the affine curve

$$2y^2 = 1 - 17x^4.$$

Later, Selmer [Se] gave examples of diagonal plane cubic curves (also of genus 1) violating the Hasse principle, including

$$3x^3 + 4y^3 + 5z^3 = 0$$

in $\mathbf{P}^2$.

O'Neil in [O'N, §6.5] constructs an interesting example of an algebraic *family* of genus 1 curves each having $\mathbf{Q}_p$-points for all $p \leq \infty$. Some fibers in her family violate the Hasse principle, by failing to have a $\mathbf{Q}$-point. In other words, these fibers represent nonzero elements of the Shafarevich-Tate groups of their Jacobians.

In [CP], Colliot-Thélène and the present author prove, among other things, the existence of non-isotrivial families of genus 1 curves over the base $\mathbf{P}^1$, smooth over a dense open subset, such that the fiber over *each* rational point of $\mathbf{P}^1$ is a smooth plane cubic violating the Hasse principle. In more concrete terms, this implies that there exists a family of plane cubics depending on a parameter t, such that the j-invariant is a non-constant function of t, and such that substituting *any* rational number for t results in a smooth plane cubic over $\mathbf{Q}$ violating the Hasse principle.

Date: October 19, 1999.

This research was supported by National Science Foundation grant DMS-9801104, an Alfred P. Sloan Fellowship, and a David and Lucile Packard Fellowship.

The purpose of this paper is to produce an explicit example of such a family. Our example, presented as a family of cubic curves in $\mathbf{P}^2$ with homogeneous coordinates x, y, z, is

$$5x^3 + 9y^3 + 10z^3 + 12\left(\frac{t^{12} - t^4 - 1}{t^{12} - t^8 - 1}\right)^3 (x + y + z)^3 = 0.$$

2. The cubic surface construction

Let us review briefly the construction in [CP]. Swinnerton-Dyer [SD] proved that there exists a smooth cubic surface V in $\mathbf{P}^3$ over $\mathbf{Q}$ violating the Hasse principle; choose one. If L is a line in $\mathbf{P}^3$ meeting V in exactly 3 geometric points, and W denotes the blowup of V along $V \cap L$, then projection from L induces a fibration $W \to \mathbf{P}^1$ whose fibers are hyperplane sections of V. Moreover, if L is sufficiently general, then $W \to \mathbf{P}^1$ will be a Lefschetz pencil, meaning that the only singularities of fibers are nodes. In fact, for most L, all fibers will be either smooth plane cubic curves, or cubic curves with a single node.

For some $N \geq 1$, the above construction can be done with models over $\operatorname{Spec} \mathbf{Z}[1/N]$ so that for each prime $p \nmid N$, reduction mod p yields a family of plane cubic curves each smooth or with a single node. One then proves that if $p \nmid N$, each fiber above an $\mathbf{F}_p$-point has a smooth $\mathbf{F}_p$-point, so Hensel's Lemma constructs a $\mathbf{Q}_p$-point on the fiber W_t of $W \to \mathbf{P}^1$ above any $t \in \mathbf{P}^1(\mathbf{Q})$.

There is no reason that such W_t should have $\mathbf{Q}_p$-points for $p|N$, but the existence of $\mathbf{Q}_p$-points on V implies that at least for t in a nonempty p-adically open subset U_p of $\mathbf{P}^1(\mathbf{Q}_p)$, $W_t(\mathbf{Q}_p)$ will be nonempty. We obtain the desired family by base-extending $W \to \mathbf{P}^1$ by a rational function $f : \mathbf{P}^1 \to \mathbf{P}^1$ such that $f(\mathbf{P}^1(\mathbf{Q}_p)) \subseteq U_p$ for each $p|N$.

More details of this construction can be found in [CP].

3. Lemmas

Lemma 1. *Let V be a smooth cubic surface in $\mathbf{P}^3$ over an algebraically closed field k. Let L be a line in $\mathbf{P}^3$ intersecting V in exactly 3 points. Let W be the blowup of V at these points. Let $W \to \mathbf{P}^1$ be the fibration of W by plane cubics induced by the projection $\mathbf{P}^3 \setminus L \to \mathbf{P}^1$ from L. Assume that some fiber of $\pi : W \to \mathbf{P}^1$ is smooth. Then at most 12 fibers are singular, and if there are exactly 12, each is a nodal plane cubic.*

Proof. Let p be the characteristic of k, and choose a prime $\ell \neq p$. Let

$$\chi(V) = \sum_{i=0}^{2 \dim V} (-1)^i \dim_{\mathbf{F}_\ell} \mathrm{H}^i_{\text{ét}}(V, \mathbf{F}_\ell)$$

denote the Euler characteristic. Since V is isomorphic to the blowup of $\mathbf{P}^2$ at 6 points ([Ma, Theorem 24.4], for example),

$$\chi(V) = \chi(\mathbf{P}^2) + 6 = 3 + 6 = 9.$$

Since W is the blowup of V at 3 points,

$$\chi(W) = \chi(V) + 3 = 9 + 3 = 12.$$

On the other hand, combining the Leray spectral sequence

$$\mathrm{H}^p(\mathbf{P}^1, \mathrm{R}^q \pi_* \mathbf{F}_\ell) \implies \mathrm{H}^{p+q}(W, \mathbf{F}_\ell)$$

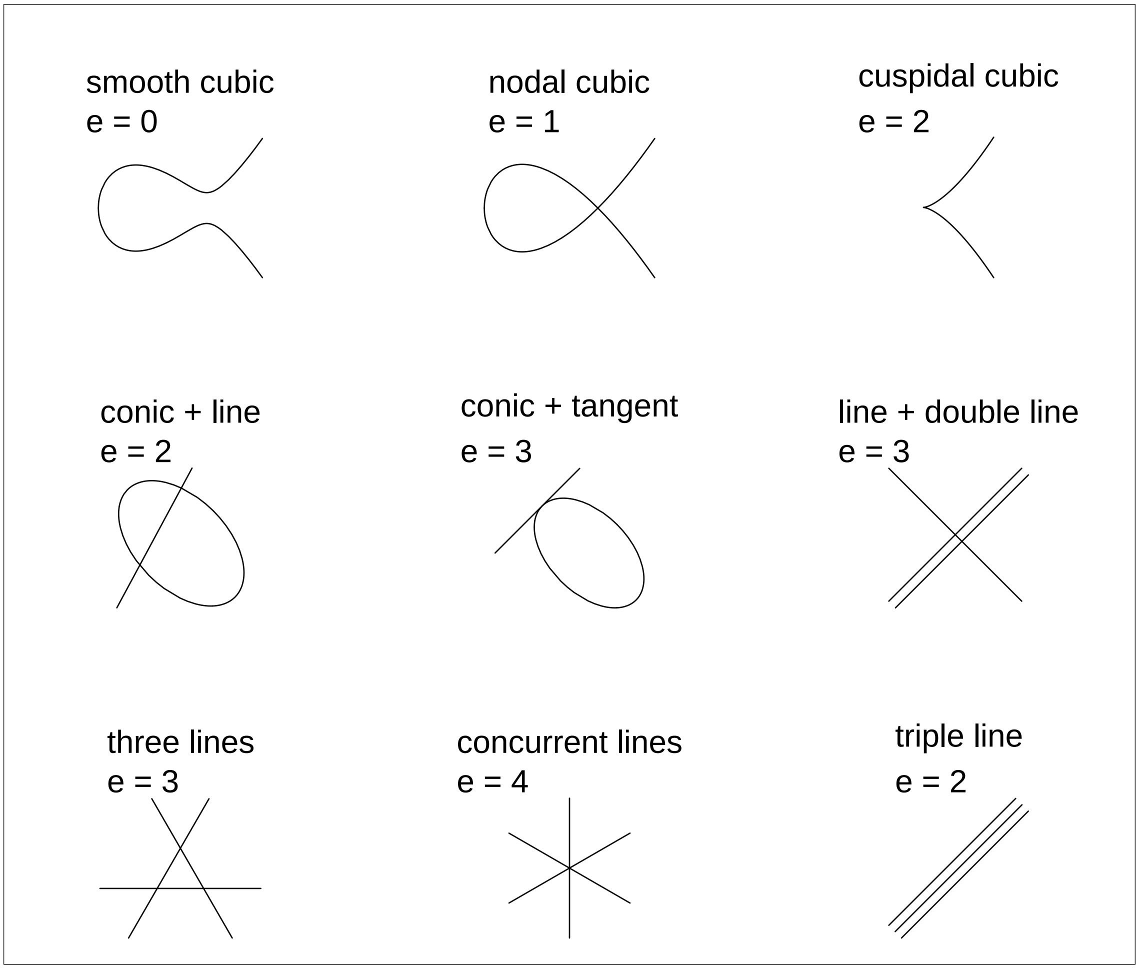

FIGURE 1. Plane cubic curves with their Euler characteristics.

with the Grothendieck-Ogg-Shafarevich formula ([Ra, Théorème 1] or [Mi, Theorem 2.12]) yields

$$\chi(W) = \chi(W_\eta)\,\chi(\mathbf{P}^1) + \sum_{t \in \mathbf{P}^1(k)} \left[\chi(W_t) - \chi(W_\eta) - \mathrm{sw}_t(\mathrm{H}^*_{\text{ét}}(W_\eta, \mathbf{F}_\ell))\right], \tag{1}$$

where W_η is the generic fiber, W_t is the fiber above t, and

$$\mathrm{sw}_t(\mathrm{H}^*_{\text{ét}}(W_\eta, \mathbf{F}_\ell)) := \sum_{i=0}^{2} (-1)^i \,\mathrm{sw}_t(\mathrm{H}^i_{\text{ét}}(W_\eta, \mathbf{F}_\ell))$$

is the alternating sum of the Swan conductors of $\mathrm{H}^i_{\text{ét}}(W_\eta, \mathbf{F}_\ell)$ considered as a representation of the inertia group at t of the base $\mathbf{P}^1$. Since W_η is a smooth curve of genus $g = 1$, $\chi(W_\eta) = 2 - 2g = 0$. If $t \in \mathbf{P}^1(k)$ is such that W_t is smooth, then all terms within the brackets on the right side of (1) are 0, so the sum is finite. The Swan conductor of

$$\mathrm{H}^0_{\text{ét}}(W_\eta, \mathbf{F}_\ell) \cong \mathrm{H}^2_{\text{ét}}(W_\eta, \mathbf{F}_\ell) \cong \mathbf{F}_\ell$$

is trivial. Hence (1) becomes

$$12 = \sum_{t\colon W_t \text{ is singular}} \left[\chi(W_t) + \mathrm{sw}_t(\mathrm{H}^1_{\text{ét}}(W_\eta, \mathbf{F}_\ell))\right],$$

Since $\mathrm{sw}_t(\mathrm{H}^1_{\text{ét}}(W_\eta, \mathbf{F}_\ell))$ is a dimension, it is nonnegative, so the lemma will follow from the following claim: if W_t is singular, $\chi(W_t) \geq 1$ with equality if and only if W_t is a nodal cubic. To prove this, we enumerate the combinatorial possibilities for a plane cubic, corresponding to the degrees of the factors of the cubic polynomial: see Figure 1. The Euler characteristic for each, which is unchanged if we pass to the associated reduced scheme C, is computed using the formula

$$\chi(C) = \sum_i (2 - 2g_{\tilde{C}_i}) + \#C_{\text{sing}} - \#\alpha^{-1}(C_{\text{sing}}), \tag{2}$$

where $\alpha : \tilde{C} \to C$ is the normalization of C, $g_{\tilde{C}_i}$ is the genus of the i-th component of $\tilde{C}$, and C_{sing} is the set of singular points of C. For example, for the "conic + tangent," formula (2) gives

$$3 = \sum_{i=1}^{2} (2 - 2 \cdot 0) + 1 - 2.$$

□

Lemma 2. *If $F(x, y, z) \in \mathbf{F}_p[x, y, z]$ is a nonzero homogeneous cubic polynomial such that F does not factor completely into linear factors over $\overline{\mathbf{F}}_p$, then the subscheme X of $\mathbf{P}^2$ defined by $F = 0$ has a smooth $\mathbf{F}_p$-point.*

Proof. The polynomial F must be squarefree, since otherwise F would factor completely. Hence X is reduced. If X is a smooth cubic curve, then it is of genus 1, and $X(\mathbf{F}_p) \neq \emptyset$ by the Hasse bound.

Otherwise, enumerating possibilities as in Figure 1 shows that X is a nodal or cuspidal cubic, or a union of a line and a conic. The Galois action on components is trivial, because when there is more than one, the components have different degrees. There is an open subset of X isomorphic over $\mathbf{F}_p$ to $\mathbf{P}^1$ with at most two geometric points deleted. But $\#\mathbf{P}^1(\mathbf{F}_p) \geq 3$, so there remains a smooth $\mathbf{F}_p$-point on X. □

4. The example

We will carry out the program in Section 2 with the cubic surface

$$V : \; 5x^3 + 9y^3 + 10z^3 + 12w^3 = 0$$

in $\mathbf{P}^3$. Cassels and Guy [CG] proved that V violates the Hasse principle. Let L be the line $x + y + z = w = 0$. The intersection $V \cap L$ as a subscheme of $L \cong \mathbf{P}^1$ with homogeneous coordinates x, y is defined by

$$5x^3 + 9y^3 - 10(x + y)^3,$$

which has discriminant $242325 = 3^3 \cdot 5^2 \cdot 359 \neq 0$, so the intersection consists of three distinct geometric points. This remains true in characteristic p, provided that $p \notin \{3, 5, 359\}$.

The projection $V \dashrightarrow \mathbf{P}^1$ from L is given by the rational function $u := w/(x+y+z)$ on V. Also, W is the surface in $\mathbf{P}^3 \times \mathbf{P}^1$ given by the $((x,y,z,w);(u_0,u_1))$-bihomogeneous equations

$$\begin{aligned} W:\ 5x^3+9y^3+10z^3+12w^3 &= 0 \\ u_0 w &= u_1(x+y+z). \end{aligned} \tag{3}$$

The morphism $W \to \mathbf{P}^1$ is simply the projection to the second factor, and the fiber W_u above $u \in \mathbf{Q} = \mathbf{A}^1(\mathbf{Q}) \subseteq \mathbf{P}^1(\mathbf{Q})$ can also be written as the plane cubic

$$W_u:\ 5x^3+9y^3+10z^3+12u^3(x+y+z)^3 = 0. \tag{4}$$

The dehomogenization

$$h(x,y) = 5x^3+9y^3+10+12u^3(x+y+1)^3,$$

defines an affine open subset in $\mathbf{A}^2$ of W_u. Eliminating x and y from the equations

$$h = \frac{\partial h}{\partial x} = \frac{\partial h}{\partial y} = 0$$

shows that this affine variety is singular when $u \in \overline{\mathbf{Q}}$ satisfies

$$2062096u^{12}+6065760u^9+4282200u^6+999000u^3+50625 = 0. \tag{5}$$

The fiber above $u = 0$ is smooth, so by Lemma 1, the 12 values of u satisfying (5) give the *only* points in $\mathbf{P}^1(\overline{\mathbf{Q}})$ above which the fiber W_u is singular, and moreover each of these singular fibers is a nodal cubic. The polynomial (5) is irreducible over $\mathbf{Q}$, so W_u is smooth for all $u \in \mathbf{P}^1(\mathbf{Q})$.

The discriminant of (5) is $2^{146} \cdot 3^{92} \cdot 5^{50} \cdot 359^4$. Fix a prime $p \notin \{2,3,5,359\}$, and a place $\overline{\mathbf{Q}} \dashrightarrow \overline{\mathbf{F}}_p$. The 12 singular u-values in $\mathbf{P}^1(\overline{\mathbf{Q}})$ reduce to 12 distinct singular u-values in $\mathbf{P}^1(\overline{\mathbf{F}}_p)$ for the family $\overline{W} \to \mathbf{P}^1$ defined by the two equations (3) over $\overline{\mathbf{F}}_p$. Moreover, the fiber above $u=0$ is smooth in characteristic p. By Lemma 1, all the fibers of $\overline{W} \to \mathbf{P}^1$ in characteristic p are smooth plane cubics or nodal plane cubics. By Lemma 2 and Hensel's Lemma, W_u has a $\mathbf{Q}_p$-point for all $u \in \mathbf{P}^1(\mathbf{Q}_p)$.

Proposition 3. *If $u \in \mathbf{Q}$ satisfies $u \equiv 1 \pmod{p\mathbf{Z}_p}$ for $p \in \{2,3,5\}$ and $u \in \mathbf{Z}_{359}$, then the fiber W_u has a $\mathbf{Q}_p$-point for all completions $\mathbf{Q}_p$, $p \le \infty$.*

Proof. Existence of real points is automatic, since W_u is a plane curve of odd degree. Existence of $\mathbf{Q}_p$-points for $p \notin \{2,3,5,359\}$ was proved just above the statement of Proposition 3.

Consider $p = 359$. A Gröbner basis calculation shows that there do not exist a_1, a_2, b_1, b_2, c_1, c_2, $\overline{u} \in \overline{\mathbf{F}}_{359}$ such that

$$5x^3+9y^3+10z^3+12\overline{u}^3(x+y+z)^3 \tag{6}$$

and

$$(5x+a_1y+a_2z)(x+b_1y+b_2z)(x+c_1y+c_2z)$$

are identical. Hence Lemma 2 applies to show that for any $\overline{u} \in \mathbf{F}_{359}$, the plane cubic defined by (6) over $\mathbf{F}_{359}$ has a smooth $\mathbf{F}_{359}$-point, and Hensel's Lemma implies that W_u has a $\mathbf{Q}_{359}$-point at least when $u \in \mathbf{Z}_{359}$.

When $u \equiv 1 \pmod{5\mathbf{Z}_5}$, the curve reduced modulo 5,

$$\overline{W}_{\overline{u}}:\ 4y^3+2(x+y+z)^3 = 0,$$

consists of three lines through $P := (1 : 0 : -1) \in \mathbf{P}^2(\mathbf{F}_5)$, so it does not satisfy the conditions of Lemma 2, but one of the lines, namely $y = -2(x+y+z)$, is defined over $\mathbf{F}_5$, and every $\mathbf{F}_5$-point on this line except P is smooth on $\overline{W}_{\overline{u}}$. Hence W_u has a $\mathbf{Q}_5$-point.

The same argument shows that W_u has a $\mathbf{Q}_2$-point whenever $u \equiv 1 \pmod{2\mathbf{Z}_2}$, since the curve reduced modulo 2 is $x^3 + y^3 = 0$, which contains $x + y = 0$.

Finally, when $u \equiv 1 \pmod{3\mathbf{Z}_3}$, the point $(1 : 2 : 1)$ satisfies the equation (4) modulo 3^2, and Hensel's Lemma gives a point $(x_0 : 2 : 1) \in W_u(\mathbf{Q}_3)$ with $x_0 \equiv 1 \pmod{3\mathbf{Z}_3}$. This completes the proof. □

We now seek a non-constant rational function $\mathbf{P}^1 \to \mathbf{P}^1$ that maps $\mathbf{P}^1(\mathbf{Q}_p)$ into $1 + p\mathbf{Z}_p$ for $p \in \{2, 3, 5\}$ and into $\mathbf{Z}_{359}$ for $p = 359$. For $p \in \{2, 3, 5\}$, the rational function $v = t^4$ maps $t \in \mathbf{P}^1(\mathbf{F}_p)$ into $\{0, 1, \infty\}$, and

$$u = \frac{v^3 - v - 1}{v^3 - v^2 - 1}$$

maps any $v \in \{0, 1, \infty\}$ to 1. Moreover $u \neq \infty$ for $v \in \mathbf{P}^1(\mathbf{F}_{359})$. Therefore, for $t \in \mathbf{P}^1(\mathbf{Q})$, the value of

$$u = \frac{t^{12} - t^4 - 1}{t^{12} - t^8 - 1}$$

satisfies the local conditions in Proposition 3.

Substituting into (4), we see that

$$X_t : \ 5x^3 + 9y^3 + 10z^3 + 12\left(\frac{t^{12} - t^4 - 1}{t^{12} - t^8 - 1}\right)^3 (x + y + z)^3 = 0 \tag{7}$$

has $\mathbf{Q}_p$-points for all $p \leq \infty$. On the other hand, $X_t(\mathbf{Q}) = \emptyset$, because $V(\mathbf{Q}) = \emptyset$. Finally, the existence of nodal fibers in the family implies as in [CP] that the j-invariant of the family has poles, and hence is non-constant.

5. The Jacobians

For $t \in \mathbf{Q}$, let E_t denote the Jacobian of X_t. Salmon in his work on invariants of a plane cubic developed formulas which were later shown in [AKMMMP] to be coefficients of a Weierstrass model of the Jacobian. We used a GP-PARI implementation of these by Fernando Rodriguez-Villegas, available electronically at ftp://www.ma.utexas.edu/pub/villegas/gp/inv-cubic.gp to show that our E_t has a Weierstrass model $y^2 = x^3 + Ax + B$ where

$$A = 145800(t^{12} - t^4 - 1)^3(t^{12} - t^8 - 1)$$

and

$$\begin{aligned} B = &-6129675t^{72} + 48660750t^{68} - 72845325t^{64} - 43776450t^{60} - 52032375t^{56} \\ &+ 392384250t^{52} - 12636000t^{48} - 198105750t^{44} - 604705500t^{40} + 229027500t^{36} \\ &+ 387518175t^{32} + 384183000t^{28} - 242872425t^{24} - 227776050t^{20} - 110899125t^{16} \\ &+ 76387050t^{12} + 41735250t^8 + 11882700t^4 - 6129675. \end{aligned}$$

Because the non-existence of rational points on V is explained by a Brauer-Manin obstruction, Section 3.5 and in particular Proposition 3.5 of [CP] show that there exists a *second*

family of genus 1 curves Y_t with the same Jacobians such that the Cassels-Tate pairing satisfies $\langle X_t, Y_t \rangle = 1/3$ for all $t \in \mathbf{Q}$. In particular, for all $t \in \mathbf{Q}$, the Shafarevich-Tate group $Ш(E_t)$ contains a subgroup isomorphic to $\mathbf{Z}/3 \times \mathbf{Z}/3$.

Acknowledgements

I thank Ahmed Abbes for explaining the formula (1) to me. I thank also Bill McCallum and Fernando Rodriguez-Villegas, for providing Salmon's formulas for invariants of plane cubics in electronic form. The calculations for this paper were mostly done using Mathematica and GP-PARI on a Sun Ultra 2. The values of A and B in Section 5 and their transcription into LaTeX were checked by pasting the LaTeX formulas into Mathematica, plugging them into the formulas for the j-invariant from GP-PARI, and comparing the result against the j-invariant of X_t as computed directly by Mark van Hoeij's Maple package "IntBasis" at http://www.math.fsu.edu∼hoeij/compalg/IntBasis/index.html for a few values of $t \in \mathbf{Q}$.

References

[AKMMMP] S. Y. An, S. Y. Kim, D. Marshall, S. Marshall, W. McCallum, A. Perlis, *Jacobians of genus one curves*, preprint, 1999.

[CG] J. W. S. Cassels and M. J. T. Guy, *On the Hasse principle for cubic surfaces*, Mathematika **13** (1966), 111–120.

[CP] J.-L. Colliot-Thélène and B. Poonen, *Algebraic families of nonzero elements of Shafarevich-Tate groups*, to appear in J. Amer. Math. Soc.

[Lin] C.-E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, Thesis, University of Uppsala, 1940.

[Ma] Yu. I. Manin, *Cubic forms*, Translated from the Russian by M. Hazewinkel, Second edition, North-Holland, Amsterdam, 1974.

[Mi] J. Milne, *Étale cohomology*, Princeton Univ. Press, Princeton, N.J., 1980.

[O'N] C. O'Neil, *Jacobians of curves of genus one*, Thesis, Harvard University, 1999.

[Ra] M. Raynaud, *Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes*, Séminaire Bourbaki, Exposé **286** (1965).

[Re] H. Reichardt, *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen*, J. Reine Angew. Math. **184** (1942), 12–18.

[Se] E. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362 and **92** (1954), 191–197.

[SD] H. P. F. Swinnerton-Dyer, *Two special cubic surfaces*, Mathematika **9** (1962), 54–56.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA

E-mail address: `poonen@math.berkeley.edu`